A Case of Trapeza

Bjorn Persson

Trapeza AB, Stockholm, Sweden
`bjorn@finit.nu`

1 The background

Trapeza is a Swedish startup company providing a solution for creating trust, transparency and facilitating electronic transactions. The principles on which the business is built are security, integrity and transparency. Around the basic function of being able to exchange personal information in a safe and controlled manner, the service will offer various forms of analysis, decision support and mediation of services. Trapeza also offers the management of personal information to meet the requirements of the GDPR in providing the individual with access to information about the treatment and legal basis for it.

Trapeza is a product and service company but not primarily a Fintech company but rather a provider of secure information. The company will initially launch its services in Sweden and then, it will look to extend the market to the rest of the Nordic countries before contemplating offering the service in the rest of Europe.

2 The problems Trapeza is addressing

1. An individual's data is seen as a commodity that can be owned and traded, without concern for the effect on the individual
2. It is difficult for a data controller to make sure he complies with the legislation and ethical standards for data processing
3. The supervisory bodies have practical difficulties with supervising and policing abuse and fraud in the digital domain
4. The risk of suffering digital fraud and abuse for both individuals and organisations

3 The actors in the domain

- **Individuals**, who have their data processed for various reasons irrespective of if they have given their consent or not.
- **Data controllers**, actors that process data in accordance with the legislation irrespective of if they are doing so based on a legal obligation or right, contractual agreement, consent, legitimate purpose or other legal foundation.
- **Data processors**, actors that process data on behalf of a data controller who have a legal right to process data and acts in accordance with such a right.

- **Data trespassers**, actors who knowingly or unknowingly process data without a legal right or for purposes not covered by a legal right to process data.
- **Fraudsters**, actors who purposefully gains access to abuses personal data in order to commit fraud or similar crimes against another party.
- **Black hat hackers**, actors who aid and abet fraudsters and trespassers in getting access to or use data for illegitimate purposes.
- **White hat hackers**, actors who work to protect individuals, data controllers and data processors from attacks or abuse of data.

4   The solution

A service that creates trust and transparency by allowing an individual to own his own information and choose how he shares this information and with whom. The core idea is that you trust people that are ready to share as much data with you as they want from you, as well as being able to follow other actors experience of them. The idea is not to create "social scoring" but rather to allow all users to decide what level of trust they want and request from those they interact with. It shall be possible to be anonymous if you request to be so, but this would most likely render you to lack credibility for most other users until you build your credibility.

The design is based on a general separation of identify and data in such a manner that it is difficult to track and identify an individual due to the amount of transactions and possible use of data minimisation techniques.

All access to data is handled by permissioned blockchain technology that distributes encryption keys that make all data access traceable as well as possible to retract.

The service also automates the legal compliance of data handling in accordance with GDPR (general data protection regulation) and KYC (know your customer) EU regulation. The possibility to automate is a result from the individual's ownership of data and the possibility to control the flow of data between the parties.

5   The problems Trapeza faces

Trapeza is planning to use blockchain technology to ensure that transactions are validated by other parties that have access to data. An example can be the income earned from work, which is stated by the individual and then validated by the employer and the tax office. The blockchain will also be used to control the access to data by ensuring that all access to data is transparent, i.e. the keys to data are distributed through the blockchain in such a manner that only the parties that are registered ang given access can decrypt the encrypted data.

The problem is twofold, will users trust the blockchain technology to handle the security, or will it be necessary too introduce some other form of control, if so which?

Since protection against fraud is an important selling point, how can Trapeza ensure that fraud is so difficult to perpetrate that this can be claimed?